UNITED STATES DISTRICT COURT

for the

Middle District of North Carolina

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

ELECTRONIC DEVICES OBTAINED ON JUNE 19, 2017 IN A CYBER EXTORTION INVESTIGATION

Case No. 1:17mj257

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

SEE ATTACHMENT A

located in the Middle District of North Carolina, there is now concealed *(identify the person or describe the property to be seized)*:

Items constituting the evidence, contraband, fruits or instrumentalities of violations of 18 U.S.C. § 1030(a)(7)(A) and (c)(3)(A), Threatening to damage a protected computer, 18 U.S.C. § 875(b), Interstate communicating threats to persons, and 18 U.S.C. § 875(d), Interstate threats, as further described in Attachment B.

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C. § 1030(a)(7)(A),(c)(3)(A)	Threatening to damage a protected computer
18 U.S.C. § 875(b), (d)	Interstate communicating threats to persons, Interstate threats

The application is based on these facts:
(SEE ATTACHED AFFIDAVIT)

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Patrick S. Berckmiller

Applicant's signature

Patrick S. Berckmiller, Special Agent

Printed name and title

Sworn to before me and signed in my presence.

Date: 08/04/17

Judge's signature

City and state: Greensboro, North Carolina

The Honorable L. Patrick Auld, Magistrate Judge

Printed name and title

IN THE UNITED STATES DISTRICT COURT
FOR THE MIDDLE DISTRICT OF NORTH CAROLINA

IN THE MATTER OF THE SEARCH OF ELECTRONIC DEVICES OBTAINED ON JUNE 19, 2017, IN A CYBER EXTORTION INVESTIGATION	Case No. 1:17mj257

AFFIDAVIT IN SUPPORT OF AN APPLICATION FOR A SEARCH WARRANT

1. I, Patrick S. Berckmiller, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

2. I am a Special Agent of the Federal Bureau of Investigation (FBI) and has been so employed since November 1998. Since April 2016, affiant has been assigned to investigate cyber related crimes to include fraud and related activity in connection with computers. From March 1999, until April 2016, affiant was assigned to investigate foreign counterintelligence matters and theft of trade secrets crimes. Affiant received training from the FBI regarding cybercrimes, foreign counterintelligence, and theft of trade secrets, and has previously been involved in investigations involving espionage, export violations, bank robbery, kidnapping, fugitives from justice, white collar crimes, and computer crimes involving the theft of proprietary data. Most recently, I have been involved in an investigation regarding a cyber

extortion matter. As a Federal Agent, I am authorized to investigate violations of laws of the United States and to execute warrants issued under the authority of the United States.

3. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

4. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that violations of 18 U.S.C. § 1030(a)(7)(A) and (c)(3)(A), Threatening to damage a protected computer, 18 U.S.C. § 875(b), Interstate communicating threats to persons, and 18 U.S.C. § 875(d), Interstate threats (hereinafter, the "TARGET OFFENSES") have been committed by TODD MICHAEL GORI. A grand jury in the Middle District of North Carolina returned a four-count indictment on April 25, 2017, charging the aforementioned offenses in case number 1:17CR146-1, *United States v. Todd Michael Gori*. There is also probable cause to search the information described in Attachment A for evidence of the TARGET OFFENSES, as described in Attachment B.

5. I make this affidavit in support of an application for a search warrant for certain devices seized from the person of TODD MICHAEL GORI upon his arrest, specifically: one black SanDisk Cruzer Glide 16GB Thumb drive, one black SanDisk Cruzer Glide 16GB Thumb drive, one black Dell 8GB Thumb drive, one black Digipower card reader Thumb drive, one black Unirex 8GB Micro SD card, one black Toshiba 2TB External Hard drive serial Number 64EBTQAOT18B, one black Alcatel Smart Phone, one white Dell Inspiron P24T laptop computer serial number F9ZFD82, one gray Alienware P42F laptop computer serial number 2RT4M72, one black Toshiba 1TB external hard drive serial number 74EZS6XFSTT1, one gray Samsung SM-G357M Smart Phone serial number R28F90EEZXL with number 9983948587 taped on the back, one black Seagate expansion desktop 8TB hard drive serial number NA8FCKJX, one black Seagate expansion desktop 8TB hard drive serial number NA8FCHBL, one black ASUS RT-N12 Wireless N Router serial number E7IADQ002112, as further described in Attachment A, (hereinafter collectively described as the "SUBJECT DEVICES"). The applied-for warrant would authorize the forensic examination of the SUBJECT DEVICES for the purpose of identifying electronically stored data particularly described in Attachment B, in relation to an investigation involving the TARGET OFFENSES.

INTRODUCTION REGARDING COMPUTERS AND GOOGLE VOICE

6. The term "computer" means an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device, but such terms does not include an automated typewriter or typesetter, a portable held calculator, or other similar device.

7. The term "Protected Computer" means a computer that is used in or affecting interstate or foreign commerce or communication, including a computer located outside the United States that is used in a manner that affects interstate or foreign commerce of communication of the United States.

8. Google Voice is a telephony service that provides call forwarding and voicemail services, voice and text messaging, as well as U.S. and international call termination services for Google Account customers in the U.S. and Canada (Google Account customers in most other countries may only access the call termination services through the integration with Google Hangouts). The service was launched by Google on March 11, 2009. Google Voice provides a U.S. telephone number, chosen by the user from available numbers in selected area codes, free of charge to each user account. Calls to this number are forwarded to telephone numbers that each user must

configure in the account web portal. Multiple destinations may be specified that ring simultaneously for incoming calls. Service establishment requires a United States telephone number. A user may answer and receive calls on any of the ringing phones as configured in the web portal. During a received call the user may switch between the configured telephones. Google Voice users in the U.S. may place outbound calls to domestic and international destinations. Calls may be initiated from any of the configured telephones, as well as from a mobile device app, or from the account portal. As of August 2011, Google Voice users in many other countries also may place outbound calls from the web-based application to domestic and international phone numbers. Many other Google Voice services—such as voicemail, free text messaging, call history, conference calling, call screening, blocking of unwanted calls, and voice transcription to text of voicemail messages—are also available to U.S. residents. In terms of product integration, transcribed and audio voicemails, missed call notifications, and/or text messages can optionally be forwarded to an email account of the user's choice. Additionally, text messages can be sent and received via the familiar email or IM interface by reading and writing text messages in Gmail or by adding contact's phone numbers in Google Talk respectively (PC-to-Phone texting). Google Voice multi-way videoconferencing (with support for document sharing) is now integrated with Google+ Hangouts.

PROBABLE CAUSE

9. On or about April 18, 2016, Federal Bureau of Investigation Special Agent Patrick Berckmiller learned of a cyber extortion threat against TSI Healthcare, 101 Europa Drive, Suite 200, Chapel Hill, North Carolina, 27511 website: www.tsihealthcare.com, Facebook: TSI Healthcare. The following message (quoted verbatim including typographical errors) was sent through the TSI Healthcare website's "contact us" page:

-----Original Message----- From: Todd Gori [mailto:toddmichael5822@gmail.com] Sent: Monday, April 18, 2016 10:04 AM To: Info <info@tsihealthcare.com> Subject: Contact Us Page Inquiry Someone has filled out the contact us form on our contact page. Below is their information: Name: Todd Gori Practice Name: Cheryl Patterson City: Wenatchee State: Washington Email: toddmichael5822@gmail.com Phone Number: 7027010985 How Did You Hear About Us: TSI Healthcare Called Me Message Body: hello, This is cheryl thompsons son. I am giving you, TSI healthcare two choices. You either lay-off my crazy workaholic mother Cheryl Thompson and replace her with me, an operator 100x better that she is oppressing. Or I will take out your entire company along with my comrades via a cyber attack. Again you have two choices. Get ride of her and hire me. Or slowly be chipped away at until you are gone. She is a horrible operator that can only manage 2 screens with an over inflated travel budget. I fly at least 10x as many places as this loon on 1/5th of the budget.

I have petitioned for a job with you guys with her as a reference as I am a felon with computer skills and need assistance getting work as technically I have "no work history". She declines everytime and burries me even further. I even stated this straight from TSI website "Center for Generational Kinetics Best Places to Work for Millennials Top 75 Millennial Employer in the U.S. 2015" and she shunned me like I was some type of idiot. How rude of my mother. A son that has wanted to be her friend both on facebook and in real life. Most people want to run from there parents in the other direction I am trying to be this woman's friend and help here and she is busy making me cry daily and making someone with good computer skills much better then her

homeless and starving. I'm giving you guys 72 hours to respond until the attack goes full scale. There is nothing that can be done to stop the attacks. I have ran multiple penetration tests on your entire network and your company fails miserably. Again let me be clear. The only way I will work with TSI and stop the attack is to fire Cheryl Thompson (my crazy workaholic mother) and hire me and ensure I am compensated enough to keep her well sedated and normal inside a nursing home before she destroys her son like she destroyed 4 families. This is not a threat this is not a means of leverage this is saving myself and my mother and if you do not comply you can prepare for the most annoying and pesky uphill cyber battle your company has ever seen. She will also be blocked from working while the attack is taking place. If it has to take place in it's entirety as it has already begun.

10. On April 21, 2016, a Special Agent with the Federal Bureau of Investigation (FBI) along with a Detective from the Wenatchee Police Department, located GORI in Wenatchee, Washington. After informing GORI of the identity of the interviewing agent and the nature of the interview, GORI demanded an attorney. GORI then stated that he did not wish to talk and slammed the apartment door. The interviewing agent tried again to talk with GORI when GORI emerged from the apartment a short time later. GORI asked to see the investigating agent's credentials. The investigating agent showed GORI the credentials. Gori stated that he wanted to photograph the credentials and ran back into the apartment to retrieve his cell phone. The investigating agent would not allow GORI to take a picture of the credentials per FBI policy, and the attempted interview was concluded. A

strong odor consistent with marijuana was emanating from GORI's apartment.

11. On May 2, 2016, the FBI received reports from the Master Call Record of the Wenatchee Police Department (WPD), Wenatchee, Washington. A call to the WPD on February 18, 2015 identified a Todd Michael GORI, date of birth February 4, 1989, as using telephone number 702-701-0985. A call to the WPD on 01/01/2016 identified a Todd Michael GORI, date of birth February 4, 1989, using telephone number 702-701-0985. A call to the WPD on March 12, 2016, identified a Todd Michael GORI, using telephone number 702-701-0985. A call to the WPD on March 15, 2016, identified a Todd Michael GORI, date of birth February 4, 1989, as using telephone number 702-701-0985.

12. On March 1, 2017, TSI Healthcare received a phone call from an individual who identified himself as Todd GORI. That phone call reached a TSI Healthcare employee who recalled taking a prior call from GORI either earlier that month or in a month recently preceding the March 1, 2017, call. In the prior call, GORI began by stating something like. "It's Todd, I'm your worst nightmare," before asking the TSI employee to contact GORI'S mother.

When the TSI employee replied that she would do her best to get the message to GORI'S mother, GORI said that no one puts him through to her and he is down to his last $1,200.00. He said if he had to, he will buy a plane ticket and fly to North Carolina, go to a gun show, purchase a gun and come to the office and begin shooting the place up, even though he hates flying. The TSI employee recognized the following two telephone numbers being used by GORI, 509-662-8165 and 702-701-0985, when he called into TSI Healthcare. The TSI employee believes she has spoken to GORI on 10-20 occasions. As a result, TSI Healthcare felt this was a credible threat and called 911 to file a police report with the Chapel Hill Police Department, who notified the FBI.

13. On March 1, 2017, the FBI contacted the Wenatchee Police Department (WPD), Wenatchee, Washington. The WPD located GORI at his place of employment, Office Depot, and approached him in regards to making computer threats to a clinic in S. Carolina (sic). GORI said he wasn't going to make any statements about that for legal reasons. The officers told GORI not to communicate with target of the threats anymore. On the same day, the Chapel Hill Police Department, Criminal Investigations Division published a law enforcement notice to Be On the Look Out (BOLO) for Todd GORI in regards to these threats.

14. On March 30, 2017, Special Agent Berckmiller was made aware of the following additional emails which were sent to a TSI Healthcare employee from the user of email account toddmichael5822@gmail.com (shown below verbatim including typographical errors):

From: Todd Michael
<toddmichael5822@gmail.com<mailto:toddmichael5822@gmail.com>>
Date: March 30, 2017 at 8:54:27 PM MST
To: David Dickson Jr.
<ddickson@tsihealthcare.com<mailto:ddickson@tsihealthcare.com>>
Subject: Re:

a hint would be 2-5m plus benifits that should last us until we die. otherwise i am shutting you down david. i want my mother back.

On Thu, Mar 30, 2017 at 8:51 PM, Todd Michael
<toddmichael5822@gmail.com<mailto:toddmichael5822@gmail.com>> wrote:
the only way for you to stop this is to terminate my mother tomorrow with adequate compansation. no two weeks. no grace period. just terminate her and structure a comp package / check that will ensure i make it to my eath window 50-60 and she will die off peacefully with decent life.

otherwise i am shutting your company down quickly piece by piece tomorrow by dusk and there is not a damn thing your corrupt ass or your crooked as friends in the feds can do.

On Thu, Mar 30, 2017 at 8:48 PM, Todd Michael
<toddmichael5822@gmail.com<mailto:toddmichael5822@gmail.com>> wrote:
i tried to be a regular person to you and all the others. instead you assholes call the feds on me twice. instead you assholes have local PD show up to my work nearly getting me fired.

you people stole my mothers soul. my real mother. and you are stealing

pieces of mine. i sent a more detailed email to info@tsihealthcare.

if my mother is not terminated tomorrow with a generous package to ensure we are both well enough off to live the rest of our short lives (ill be lucky to live to 50 given family health issues) then you can fully expect your company to undergo serious digital issues and be very lucky to even have a digital precense online

you can call the feds all you like liek the rat you and your people are there is nothing they or you can do now.

i sit on a roof contemplating suicide tonight (again) and my own mother talks endless shit to me. Not my old mother. The new one. The one you people created. The one you people stole the soul from. The soul you are stealing from me through her.

i dont care what you think about my emails. How crazy i am. FBI or whatever. I really dont care david. If my mother is terminated without adequate compensation it will make matters even worse.

You must understand this is not an extortion attempt or a terrorist plot (nobody likes to feel powerless and extorted esp by some punk behind a pc). This is me saving my mother, myself, and what little family i have left. After you people got involved my entire family has been shattered to bits.

please ensure my mother is terminated tomorrow with adequate compensation. its the only way to stop the attack. Immediate termination with generous comp package for her services and selling her fucking soul to you people.

if i am not taken care of along with her in the compensation package then i can guarantee you pending a nuclear exlosion on all continents you epople will be working and buidling your company from all paper. you will be lucky if i let you even have a website or send a single email.

again let me make it clear to you and your corrupt friends at the FBI. I have

no interest in doing this. But you epople stole my real mother from me. Make it right or i will make it right by serviging justice against the corrupt (you and your other corrupt friends that run in vast numbers internationally)

15. On March 31, 2017, GORI made two calls to TSI Healthcare, stating he wanted to reach his mother, Cheryl Thompson. In the second call which GORI made to TSI Healthcare, he began to provide a TSI Healthcare staff member his contact information, which began with "toddmichael" and then became inaudible.

16. On April 3, 2017, GORI called TSI Healthcare and told a TSI Healthcare staff member that he wants his mother to call him on Mexican telephone number 011-52-998-883-0270.

17. On April 6, 2017, Todd GORI posted the following messages on his Facebook page:

April 6 at 11:25pm

FEDS TROLLIN HARD THATS ALL THEY KNOW #FAGGOTS

April 6 at 11:27pm

FEDS = 0 SKILL ALL TROLLS

April 6 at 11:26pm

99.9% OF FEDS ARE FLAMING COCKSUCKING CLOSETED

HOMOSEXXUALS. REMEMBER THAT

18. On April 12, 2017, GORI called TSI Healthcare, stating that he was in Mexico and his mother was able to scrape together $100.00. GORI further stated he has emails waiting from his mother, and asked TSI Healthcare staff to have his mother check her emails. He provided a call-back telephone number of 702-701-0985. GORI stated that because he was using GoogleVoice, his phone reception for incoming calls was spotty.

19. On April 13, 2017, GORI called TSI Healthcare from "his other number" (no further information), and left a message asking to please get a message to his mother and that he was still waiting on emails back from her.

20. On June 19, 2017, GORI was taken into custody by United States Customs and Border Protection (CBP) Officers, upon his arrival at Dallas Fort Worth International Airport, Texas, from Cancun, Mexico. GORI's arrest was pursuant to the federal arrest warrant in Middle District of North Carolina case 1:17CR146-1. A CBP Officer spoke to GORI in the normal course of processing upon arrest. When the officer asked GORI how long he had been in Mexico, GORI said he had been in Mexico for about three months, and was trying to establish residency there. The officer relayed this

information to an FBI Special Agent later that day in person. At the time of his arrest, GORI was in possession of the SUBJECT DEVICES.

21. Your Affiant knows, through his training, experience, and from discussions with other law enforcement officers who have investigated cyber extortion matters, that computers and mobile telephones are capable of connecting to the Internet. A computer can also be used as a telephone with applications such as Google Voice, utilizing voice over Internet Protocol (VOIP). The affiant also knows that routers contain logs that store information about the connectivity of devices to specific networks which can provide the location through an Internet Protocol (IP) address. Your Affiant also knows that SUBJECT DEVICES are capable of storing evidence related to this cyber extortion matter and that SUBJECT DEVICES are each capable of retaining electronic information for a long period of time.

22. The SUBJECT DEVICES are currently in the lawful possession of the Federal Bureau of Investigation and stored at 1801 Stanley Road, Suite 400, Greensboro, North Carolina. All of the SUBJECT DEVICES were seized from Todd Michael GORI at the time of his arrest on June 19, 2017.

TECHNICAL TERMS

23. Based on my training and experience, I use the following technical terms to convey the following meanings:

a. Wireless telephone: A wireless telephone (or mobile telephone, or cellular telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional "land line" telephones. A wireless telephone usually contains a "call log," which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic "address books;" sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones

may also include global positioning system ("GPS") technology for determining the location of the device.

b. IP Address: An Internet Protocol address (or simply "IP address") is a unique numeric address used by computers on the Internet. An IP address is a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet computer must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.

c. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

d. Denial of Service: In computing, a denial-of-service attack (DoS attack) is a cyber-attack where the perpetrator seeks to make a

machine or network resource unavailable to its intended users by temporarily or indefinitely disrupting services of a host connected to the Internet. Denial of service is typically accomplished by flooding the targeted machine or resource with superfluous requests in an attempt to overload systems and prevent some or all legitimate requests from being fulfilled. In a distributed denial-of-service attack (DDoS attack), the incoming traffic flooding the victim originates from many different sources. This effectively makes it impossible to stop the attack simply by blocking a single source. A DoS or DDoS attack is analogous to a group of people crowding the entry door or gate to a shop or business, and not letting legitimate parties enter into the shop or business, disrupting normal operations.

e. Malware: short for malicious software, is an umbrella term used to refer to a variety of forms of hostile or intrusive software, including computer viruses, worms, trojan horses, ransomware, spyware, adware, scareware, and other malicious programs. It can take the form of executable code, scripts, active content, and other software. Malware is defined by its malicious intent, acting against the requirements

of the computer user - and so does not include software that causes unintentional harm due to some deficiency.

24. Based on my training, experience, and research, and from consulting the other law enforcement officers who have technical examination experience, I know that the SUBJECT DEVICES have capabilities that allow them to serve as an electronic storage device(s), electronic devices capable of connecting to the Internet, and/or electronic devices capable of communicating with other electronic devices via email, text messaging, voice and chatting.

ELECTRONIC STORAGE AND FORENSIC ANALYSIS

25. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored indefinitely on devices which can access the Internet. This information can often be recovered with forensics tools.

26. There is probable cause to believe that data stored on the SUBJECT DEVICES is likely to still be stored there, for at least the following reasons:

a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

c. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how a computer has been used, what it has

been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

e. Forensic evidence. As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the SUBJECT DEVICES were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence might be on the SUBJECT DEVICES because:

f. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created.

g. Forensic evidence on a device can also indicate who has used or controlled the device. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence.

h. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.

i. The process of identifying the exact electronically stored information on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

j. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

k. I know that when an individual uses an electronic device, the individual's electronic device will generally serve both as an instrumentality for committing the crime, and also as a storage medium for evidence of the crime. The electronic device is an instrumentality of the crime because it is used as a means of committing the criminal offense. The electronic device is also likely to be a storage medium for evidence of crime. From my training and experience, I believe that an electronic device used to commit a crime of this type may contain: data that is evidence of how the electronic device was used; data that was sent or received; and other records that indicate the nature of the offense.

l. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the SUBJECT DEVICES consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the SUBJECT DEVICES to human inspection in order to determine whether they are evidence described by the warrant.

m. *Manner of execution.* Because this warrant seeks only permission to examine the SUBJECT DEVICES already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

CONCLUSION

27. I submit that this affidavit supports probable cause for a search warrant authorizing the examination of the SUBJECT DEVICES described

in Attachment A to seek the items described in Attachment B.

Respectfully submitted,

Patrick S. Berckmiller
Special Agent
Federal Bureau of Investigation

Subscribed and sworn to before me on August 4, 2017

THE HONORABLE L. PATRICK AULD
UNITED STATES MAGISTRATE JUDGE
MIDDLE DISTRICT OF NORTH CAROLINA

ATTACHMENT A

Property to Be Searched

The property to be searched (SUBJECT DEVICES) consist of:

1. One black SanDisk Cruzer Glide 16GB Thumb drive
2. One black SanDisk Cruzer Glide 16GB Thumb drive
3. One black Dell 8GB Thumb drive
4. One black Digipower card reader Thumb drive
5. One black Unirex 8GB Micro SD card
6. One black Toshiba 2TB External Hard drive serial Number 64EBTQAOT18B
7. One black Alcatel Smart Phone
8. One white Dell Inspiron P24T laptop computer serial number F9ZFD82
9. One gray Alienware P42F laptop computer serial number 2RT4M72
10. One black Toshiba 1TB external hard drive serial number 74EZS6XFSTT1
11. One gray Samsung SM-G357M Smart Phone serial number R28F90EEZXL with number 9983948587 taped on the back
12. One black Seagate expansion desktop 8TB hard drive serial number NA8FCKJX

13. One black Seagate expansion desktop 8TB hard drive serial number NA8FCHBL

14. One black ASUS RT-N12 Wireless N Router serial number E7IADQ002112

The SUBJECT DEVICES are currently in the possession of the Federal Bureau of Investigation Greensboro, North Carolina, and stored at 1801 Stanley Road, Suite 400, Greensboro, North Carolina 27407.

ATTACHMENT B

1. All records on or in the SUBJECT DEVICES described in Attachment A that relate to violations of Title 18, United States Code, Section 1030 (a) (7) (A) and (c) (3) (A), Threatening to damage a protected computer, 18 United States Code, Section 875 (b) Interstate communicating threats to persons and 18 United States Code, Section 875 (d) Interstate threats and involve Todd Michael GORI, in the form of:

    a. Any form of communication directly or indirectly involving TSI Healthcare;

    b. Threats in the form of documents, emails, voice recordings, texts, photos, images, scans;

    c. Information referencing employees of TSI Healthcare, (including names, addresses, phone numbers, email addresses, or any other identifying information);

    d. Photographs, images, building plans, maps, directions, web browsing history, search engine data, or identifying information regarding the TSI Healthcare facility.

    e. Information regarding the TSI Healthcare's website, webportal, employee log in portal, Facebook page, or other social media accounts.

f. Hacking tools, malware, ransomware, Denial of Service (DoS), Distributed Denial of Service (DDOS) software or services or discussion of such tools which can be used in order to gain unauthorized access or deny access to a protected computer.

g. Manifesto, or any other document relating to the use or desire of violence directed at others.

h. Any information related to the research, planning, purchase, preparation or use of firearms in the commission of an act of violence.

i. Any information relating to acquiring firearms at gun shows.

2. Evidence of user attribution showing who used or owned the SUBJECT DEVICES at the time the things described in this warrant were created, edited, or deleted, such as logs, phonebooks, text messages, voice calls, recordings, saved usernames and passwords, documents, and browsing history.

3. As used above, the terms "records" and "information" include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.